ABSTRACT

In at least one implementation, described herein, P and $Q_1,...,Q_n$ are public points on an elliptic curve over a finite field, but the ratios of Q_i to P are private. Those ratios are the components (α_1, ..., α_n) of a private key, where $Q_i = \alpha_i P$. This implementation generates short digital ciphers (i.e., signatures), at least in part, by mapping a message M to a point T on the elliptic curve and then scaling that point T based upon the private key α to get S. At least one other implementation, described herein, verifies those ciphers by comparing pairing values of two pairs, where one pair is the public point P and the scaled point S and another pair is public Q and the point T. This implementation tests whether $\log(Q)/\log(P) = \log(S)/\log(T)$, without computing any elliptic curve discrete logarithm directly.